Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 8, 2018

RaghunadhaReddy. Pocha, Ed.
ChandraShekar. Jamadarkhani, Ed.
Satyanarayana. Danda
Nishad. M
Nagappa. Chinnannavar
Cisco Systems
December 5, 2017

Virtual NAS (vNAS) Support for DNAS
draft-bng-radext-virtual-nas-for-dnas-01

Abstract

This specification defines a framework for interacting North bound (AAA/Policy) servers of the Client resides in Cloud and/or Distributed Network environment with High-Availability to achieve fewer use-cases. First, NAS Client resides in Cloud or Virtualized or Distributed Network Access System to perform Authorization, Authentication and Accounting procedures with AAA Servers. Second, AAAA/Policy Servers provide dynamic policy information for subscribers of supporting in NAS Clients resides in Cloud or Virtualized or Distributed Network environment. Finally, Handling of Accounting related issues in better way for subscribers supported in Cloud or Virtualized or Distributed Network environment under High-Available conditions.

Table of Contents

1. Introduction

In a Distributed Network Access Systems (DNAS) of containing network elements of having interaction with AAA systems to perform Authorization, authentication and Accounting (AAA) operations for end-users. Each Distributed Network Access Element (DNAE) in DNAS acts as NAS client which will interact with AAA server using Distributed Network Access Controller?s (DNAC?s) connecting parameters using source-ip-address, source-port and shared-secret. All DNAEs in DNAS shall interact with DNAC locally either using proprietary mechanism or custom defined environment which will avoid DNAEs to be exposed to AAA Server and are morphed by DNAC identify parameters. Phenomenally this will leads to challenges for AAA Servers to authorize end-users based on NAS-Client parameters and difficult to maintain accounting records as unware complete NAS-Client information. And also, it?s difficult for DNAC to segregate and distribute received Dynamic Author requests for respective users from AAA Servers towards DNAEs. Under high availability conditions for DNAS located geographically or DNAEs located in DNAS, AAA Servers unware to maintain accounting records for node or element failures. A mechanism should exist to intimate AAA Server about DNAS/DNAE failure or recovering status by including relevant Radius Attributes in Accounting Records. This document outlines the problems encountered in DNAS for AAA operations, Policy exchange and high available scenarios. Furthermore, the document proposes solutions or possible approaches of related to elements in Distributed Network systems. The purpose of this document is to introduce virtual-NAS (vNAS) and other Radius attributes as solution to help Distributed Network Systems to solve above said problems by including values in Authentication, Accounting and dynamic author attributes. With this approach, the goal is to allow the construction of standardized, interoperable implementations to allow DNAS in data centers or in cloud. Section 1.2 gives terminology and overview of DNAS and respective elements. Section 3 describes the problem space details. Section 4 describes Importance of vNAS in DNAS in more detail. Section 5 talks about vNAS role in AAA Server for DNAS, and rest of the sections are about other aspects of IETF draft.

1.1. Outline of the document

The document gives a high level overview of proposal. It then describes the overall solution of interacting with AAA Servers for Distributed Network Access Systems by leveraging existing or adding new Radius attributes.

1.2. General Terminology

Distributed Network Access System (DNAS): It is a physical system resides in Data Center or cloud of having one or more Control-Plane(CP) and/or Data-Plane(DP) aggregated as different/same network elements.

Distributed Network Access Element (DNAE): It is logically defined system in a physical system resides in DNAS which shall act as Control-Plane or Data-Plane.

Virtual Machine (VM): A software implementation of a physical machine that runs programs as if they were executing on a physical, Non-virtualized machine. Applications (generally) do not know they are running on a VM as opposed to running on a "bare metal" host orserver, though some systems provide a para-virtualization environment that allows an operating system or application to be aware of the presence of virtualization for optimization purposes.

Virtual NAS (vNAS): This is a string that uniquely identifies a Distributed Network Element in DNAS.

Control-Plane: A software implementation of a physical machine which known to process only control packets.

Data-Plane: A virtualized based or proprietary platform based physical machine which shall process forward data packets of end-users towards core networks and vice versa.

Aggregated Control-Plane (Aggr-CP) or Proxy Control-Plane (Proxy-CP): A software implementation of a physical machine, one of the DNAE which shall act as an entry or exit point for entire DNAS and interact with AAA Server on behalf of other DNAEs in a DNAS. Proxy-CP/Aggr-CP role is superset of control-plane.

1.3. Distributed Network Access Systems

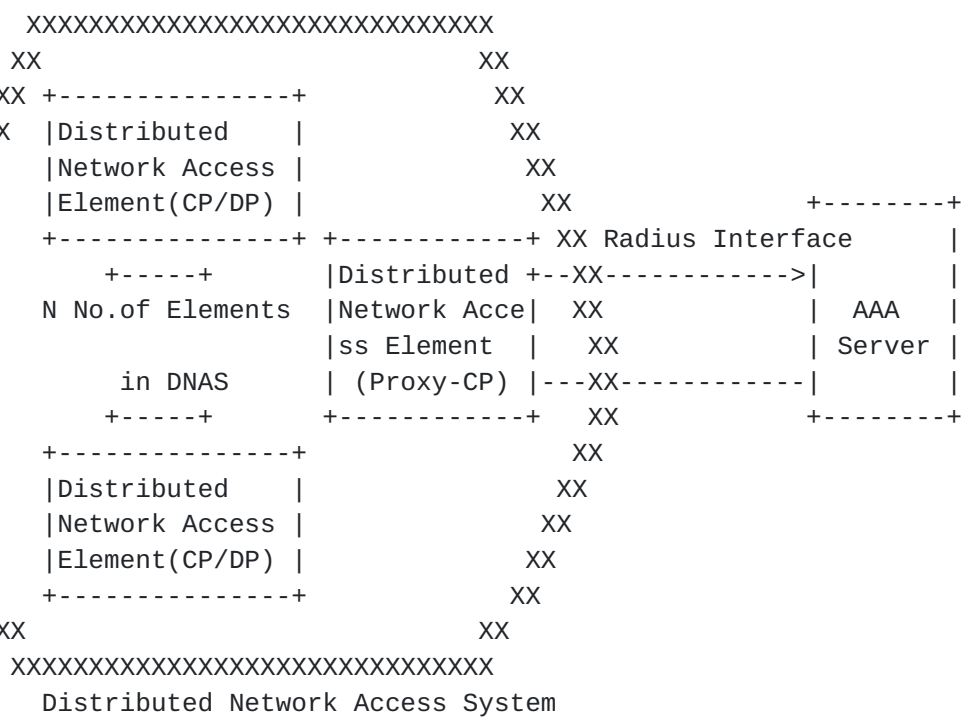

Figure 1. Interaction of DNAS with AAA Server

In Figure 1, DNAS is Distributed Network Access Sytem which shall sevice end-users in any deployment models like broadband or any celluar or Mobile Packet Core(MPC) or Evolved Packet Core(EPC) for voice, video, data services. This DNAS shall be a Prioriety hardware or Virtualized machine which is placed in Cloud or data network centers. Each DNAS shall have several DNAEs which shall serve end-users based on deployment models, these DNAEs shall act as CP-DP as single entity or each DNAE shall act as either CP or DP. In any of the model, DNAS shall maintain centralized Control-Plane(CP) which shall interact with AAA Server for AAA Operations and these CP shall be called as Proxy-CP or Aggr-CP, refered in whole document. No.of DNAEs in DNAS is purely depends on hardware architecture and resources.

1.4. Processing Dynamic Author Request in DNAS

In DNAS Architecture of consisting of several CPs to support AAA operations for end-users and assume that there is one common CP which act as a proxy and shall interact with AAA Server on behalf of all CPs as mentioned in section 1.3. Under these conditions, AAA Server may send Dynamic Author Request as per RFC 5716 without including proper NAS-Identifier of DNAE. These messages shall be cumbersome for aggregated control-plane to forward the request to respective DNAEs and today these can be achieved by broadcasting the message to

all DNAEs. This is a bottle neck for DNAS performance on handling Dynamic Author Requests. As the message is broadcasted to all respective CPs, the Proxy-CP shall wait to receive responses from respective CPs to honor the received Dynamic Author Request to AAA Server. This will provide delay for final response packet to AAA Server, which in turn degrade the overall performance of AAA interaction.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119. In this document, the characters ">>" preceding an indented line(s) indicates a statement using the key words listed above. This convention aids reviewers in quickly identifying or finding the portions of this RFC covered by these keywords.

3. Problem Areas

The following subsections describe aspects of Distributed Network Systems that pose problems for AAA Operations. Different problem aspects may arise based on the network architecture and scale along with High Availability conditions.

3.1. AAA Operations in DNAS

In DNAS Architectures, it?s always good to provide NAS client information to AAA Server while performing AAA operations to end-user. In current deployment models, NAS-IP-Address, NAS-Port and NAS-Identifier are the key attributes which will specify the NAS-Client information. Having these attributes right from beginning of transactions (from Authorization/Accounting) shall help to the end-users from billing perspective and also policy enforcement.

In DNAS Architecture, the concept of NAS-Identifier has to be elaborated to individual DNAEs so that it can meet the specifications. A methodology is defined with concept of vNAS(Virtual-NAS) under section [4] to deal with DNAS and section [6] shall define the definition of vNAS.

For Accounting-On and Accounting-Off transactions for Node UP/Down failures, inclusion of NAS-Identifier and it?s value plays a vital role as AAA Server shall keep Accounting records for on-going end-

user transactions and also helpful to push policies for existing subscribers.

3.1.1. Intimating DNAS/DNAE status to AAA Server

Today, NAS Client notify the status of the system UP/DOWN using Accounting On/Off transactions to AAA Server to inform the system credentials. Based on this information, AAA Server shall maintain this information to maintain the accounting records for end-users whenever accounting records are received from respective NAS-Client and also enforce the dynamic policies to NAS-Client using Dynamic Authorization procedures for end-users.

In a given DNAS, there is no methodology in place to intimate DNAS/ DNAE identifiers to maintain at AAA Server level to serve the above said functionality fully.

3.1.2. Dealing with AAA Operations for DNAS with High Availability

This is a high availability scenario where multiple DNASs are located geographically to serve end-users for AAA operations in N:M Redundancy model where N and M are no.of DNASs in Active-Active or Active-Standby model.

A system in DNAS with high available conditions, always has to publish system identifiers to AAA Server whenever HSRP redundancy states are changed. This mechanism shall help at AAA level to serve the NAS-Client to push dynamic policies and also to maintain the accounting records for end-users.

There are multiple ways of having DNASs under high available scenarios.

In Figure-2, the DNAEs across DNAS are in redundancy mode. That means, DNAE in DNAS-1 shall have respective redundancy mode in DNAS-2. Similarly, Aggr-CP/Proxy-CP of DNAS-1 shall have respective redundancy node another DNAS-2. The redundancy handling of Control-Plane/Data-Plane is not going to be discussed in this draft and it?s completely implementation dependent.

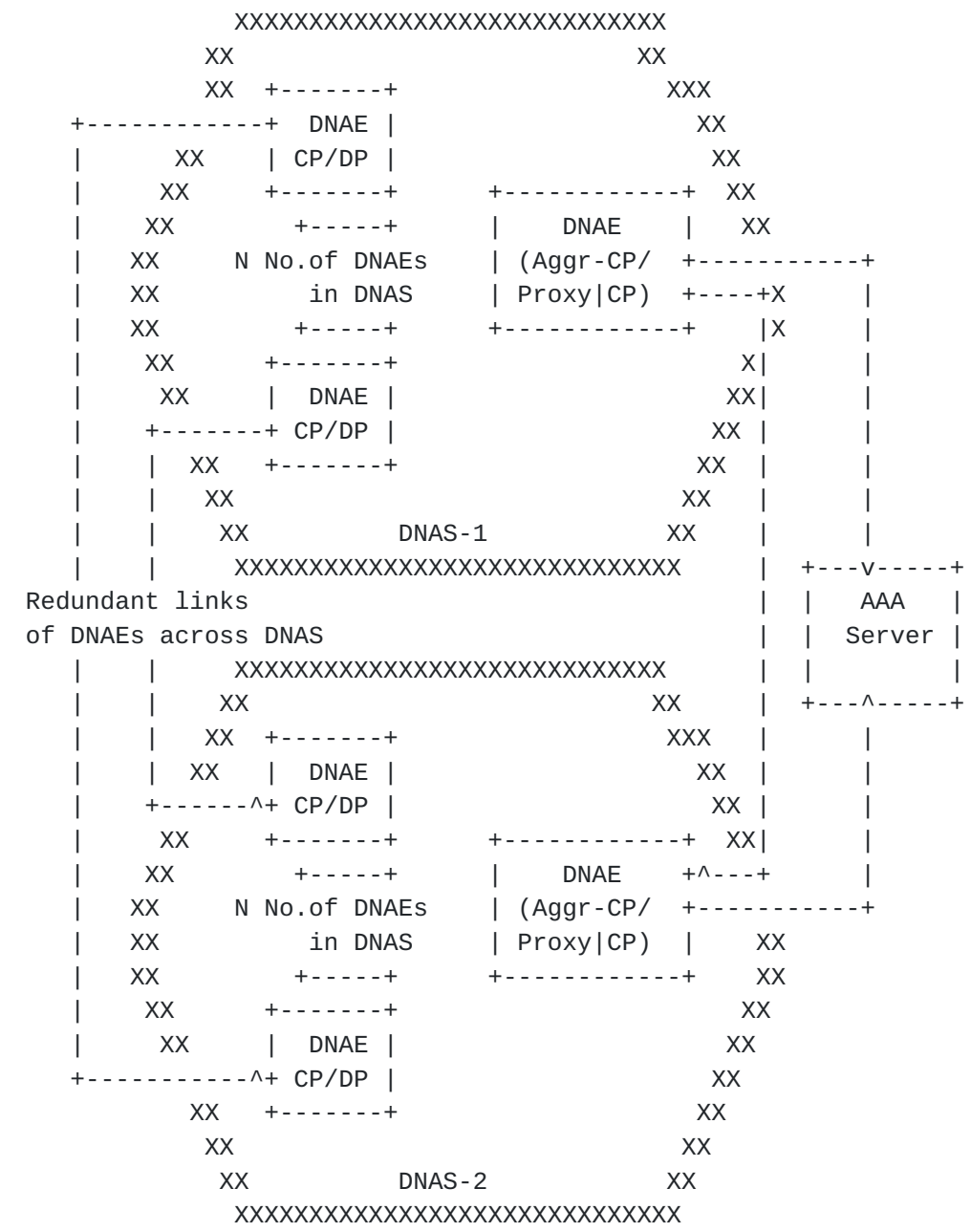

Figure 2. DNAEs across DNAS in High Available Scenarios

Unlike Figure-2 DNAS Redundancy topology, Figure-3 explains the redundancy within the DNAEs as well. Where each DNAEs have several HSRP groups which shall serve certain end-users in redundancy mode across DNAEs and DNAS. The redundancy handling of Control-Plane/ Data-Plane is not going to be discussed in this draft and it?s completely implementation dependent.

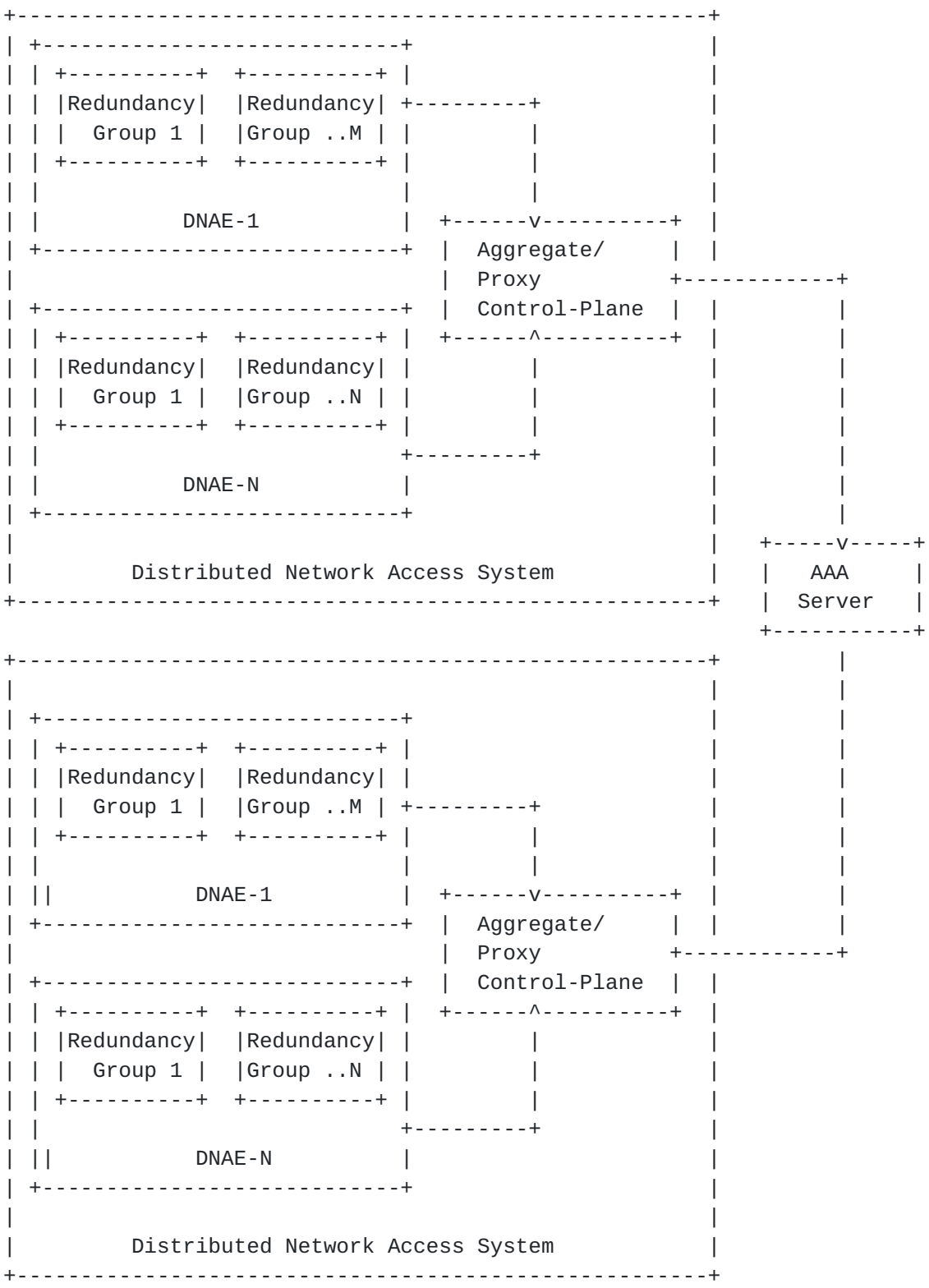

Figure 3. Redundancy Groups inside DNAEs across DNAS in HA Scenarios

For all above approaches, there is no mechanism to handling accounting records at AAA level and pushing dynamic policies across DNAS for end-users.

The following subsections describe aspects of Distributed Network Systems that pose problems for AAA Operations. Different problem aspects may arise based on the network architecture and scale along with High Availability conditions.

3.2. AAA Operations in AAA Server

AAA Server shall maintain NAS-Client information whenever respective NAS Clients are UP/DOWN so that it?s easy to push Dynamic Policies and also to maintain accounting records for end-users of respective NAS-Client based on identifiers that are received as part of Accounting On/Off messages. The same is applicable under High available conditions as explained in earlier sections.

3.2.1. Policy-Enforcement from AAA Server

In DNAS Architecture based deployment models, enforcing policies from AAA Server using Dynamic Authorization procedures are never be easy as the elements in DNAS are not much exposed to AAA Server. This will restrict AAA Server to send all Dynamic Authorization request messages to CP-Proxy of DNAS, DNAS has to broadcast those messages to all DNAEs in it. Since DNAS is going to take more time because of broadcast to it?s DNAEs, the AAA Server will continue to retransmit the Dynamic Authorization request. This will impact the performance on interactions between AAA Server and DNAS

3.2.2. Maintaining Accounting Records on AAA Server for end-users

Maintaining the accounting records with respective DNAS/DNAE element identifiers shall helpful for better billing of subscriber movement across DNAS/DNAE based on deployment models. This will also helpful to enforce new policies based on newly received DNAS/DNAE identifiers. Today, majority of deployment models are not of DNAS based and mostly maintaining accounting records are based on nas-ip-address and nas-identifier. Nas-IP-Address is unique per DNAS and there is no identifier to discriminate the individual DNAEs. This shall enforce limitation on AAA Server to achieve the actual functionality in DNAS Architecture.

4. Importance of vNAS in DNAS

vNAS is Virtual-NAS shall defined in DNAS to identify a DNAE which is included as an attribute on performing authorization, authentication and accounting transactions for end-user. This vNAS value shall help

to identifier the NAS-Client in DNAS environment for end-user so that AAA Server operations shall be easier to operate w.r.to round-trip-time and resource utilization.

4.1. Defining vNAS for DNAS

vNAS is Virtual-NAS shall defined in DNAS to identify a DNAE uniquely. As defined in Figure-1, DNAS system consists of various DNAEs which will act as control-plane and data-plane. However, there is one element which can interact with AAA Server which is known as Aggregated Control-Plane (Aggr-CP) or Proxy Control-Plane (Proxy-CP). The Proxy-CP shall provide vNAS for each DNAE uniquely in DNAS environment whenever the DNAE is spawned/booting-time. Proxy-CP shall maintain the vNAS Table of having mapping between vNAS vs DNAEs so that all AAA operations shall be unicasted to respective DNAE based on vNAS table lookup for a received vNAS value.

The aim of defining or generation of vNAS should be unique for each DNAE as this vNAS value shall be included in Radius NAS-Identifier of Radius messages. The generation of vNAS on Proxy-CP shall be done in many ways and shall vary from deployment models. The following are fewer approaches of generating the vNAS for DNAE,

1) Using DNAE naming conventions used in DNAS. 2) Using DNAE bit mapping. 3) Using DNAE Name + Boot-up TimeStamp 4) Using DNAS Name + DNAE Name + Boot-Up Timestamp. 5) Using DNAS Name + DNAE Name + Group-Id

The approach (1), (2) and (3) shall provide uniqueness within the system but not across DNASs. Approach (4) shall provide uniqueness across DNAS where AAA Server also shall identify the entire DNAE information in DNAS environment. Approach (5) shall provide vNAS uniqueness across DNAS for high availability cases where each Group-Id represents on Group when DNAEs have multiple Groups in it under high availability cases.

Approach-1, Aggr-CP/Proxy-CP DNAS shall generate DNAE name while spawning the DNAE in DNAS environment and maintain the strict mapping internally on Aggr-CP/Proxy-CP. This solution shall work for standalone systems.

Approach-2, There is no naming convention here. It?s more of like how the dynamic/static bit mapping is maintained at Aggr-CP/Proxy-CP whenever DNAE boots up. This solution shall work for standalone systems.

Approach-3, Aggr-CP/Proxy-CP of DNAS shall generate DNAE name along with Boot-UP timestamp. This shall provide more uniqueness within DNAS and good for standalone systems only.

Approach-4, Aggr-CP/Proxy-CP of DNAS shall generate DNAE name by considering the DNAS name along with Boot-UP timestamp of DNAE. This shall provide more uniqueness across DNAS and is perfect for Redundancy models across DNAS (as defined in Figure-2).

Approach-5, This use case is special use case as defined in Figure-3. Aggr-CP/Proxy-CP of DNAS shall generate vNAS by considering DNAS name, DNAE name and HSRP Group-name which shall provide more uniqueness across DNAS and is perfect for Redundancy models across DNAS.

The ultimate goal of generating vNAS is to have more uniqueness across DNAS where multiple DNAS are deployed in a network to provide services to end-users.

Based on approaches defined and network topology conditions, let the Centralized Configuration Manager provides unique vNAS to DNAEs in DNAS using NetConf/Yang.

The vNAS identifier value shall include in NAS-Identifier as defined in [4]. The generation of vNAS should fit the length values of NAS-Identifier.

4.2. vNAS for AAA Operations

DNAS shall perform AAA Operations for end-user by sending authentication, accounting messages. In all these messages, DNAS shall include NAS-IP-Address and NAS-Identifier. In a given DNAS system, there are multiple ways of interacting with AAA Server.

One of the way is, individual DNAEs shall send triggers for AAA operations internally to Proxy-CP and Proxy-CP shall send out AAA Messages after including nas-ip-address and vNAS Identifier. In this case, DNAEs are not exposed with AAA configuration parameters and complete owns of AAA messages transactions are well taken care by Proxy-CP only.

Another way of sending messages are, individual DNAEs AAA configuration i.e., DNAEs are aware of NAS-IP-Address of DNAS and AAA Server information. This will help DNAEs to include NAS-IP-Address and vNAS as NAS-Identifier in AAA messages. In this case the complete ownership of AAA message transactions are taken by individual DNAEs except Dynamic-Authorization-Requests which will be

dealt in section 4.3. Holding unique NAS-IP-Address by each DNAE is ruled out in DNAS environment.

4.3. vNAS for Dynamic Author Request Processing

AAA Server shall use Dynamic Author Requests end-user to intimate session termination by sending Disconnect-Request or pushing dynamic-policies or other much needed interim session information by sending Change-Of-Authorization to NAS-Client where the end-user AAA context is maintained which is as per [9].

Based on sections 4.2 and 5, AAA Server shall include vNAS values in NAS-Identifier of Dynamic-Authorization-Request message for end-user which are targeted to DNAEs located in DNAS where the end-user AAA Context is maintained so that request shall be processed. Since, the DNAEs doesn?t have direct interaction with AAA Server and vice versa ? the dynamic-author request messages shall sent to Proxy-CP of DNAS. The DNAS of Proxy-CP shall process the received request and look for NAS-Identifier value which is nothing but vNAS value. Proxy-CP Search for vNAS table to match the vNAS value for fetching the DNAE so that the request shall be unicasted internally to respective DNAE.

There are several ways of handling Dynamic-Author Request at Proxy-CP on DNAS. One of the approach is, Proxy-CP shall act as a message dispatcher to DNAE after vNAS lookup where proxy-cp shall not maintain any message transaction. DNAE shall respond back to DNAS as defined in section 4.2 via Proxy-CP or directly to AAA Server. Any delay of processing Proxy-CP shall keep forwarding any retransmitted messages

Another approach is, Proxy-CP can maintain the message context so that the DNAE shall respond with status of message to Proxy-CP and Proxy-CP shall send final response to AAA Server. Proxy-CP of DNAS will trigger an internal timer to wait for response message from DNAE. And also, DNAS shall silently drop any retransmitted messages received from AAA Server in this duration.

4.4. Dealing with vNAS for DNAS under High Available Scenarios

Under high availability scenarios defined in section 3.1.3, where multiple DNASs are located geographically to serve end-users for AAA operations in N:M Redundancy model where N and M are no.of DNASs are in Active-Active or Active-Standby model.

A system in DNAS with high available conditions, always has to publish system identifiers to AAA Server whenever HSRP redundancy states are changed. This mechanism shall help at AAA level to serve

the NAS-Client to push dynamic policies and also to maintain the accounting records for end-users.

Under high available conditions, DNAS shall have different NAS-IP-Address unless the AAA Server are connected core links. For any deployment case, AAA Servers are not exposed to core-link and hence, the Active/Standby DNAS shall have different NAS-IP-Address. Whenever switchover happened, OLD DNAS and respective DNAEs in it shall send Accounting-Off and Accounting-Request with Acct-Status-Type STOP for individual end-users to close outstanding accounting transactions. Similarly, the new DNAS and respective DNAEs role is exchanged i.e., Standby -> Active. The new DNAS and respective DNAEs state start sending Accounting-On and Accounting-Request with Acct-Status-Type START for individual end-users to open accounting transactions.

Updating the NAS-IP-Address in DNAS and vNAS of DNAEs with AAA Server are very import in High Availability scenarios, this shall help to push Dynamic-policies to new DNAEs directly for end-users.

5. vNAS role in AAA Server for DNAS

AAA Server shall maintain NAS-Client information whenever respective NAS Clients are UP/DOWN by receiving Accounting On/Off messages, so that it is easy to maintain accounting records for end-users belong to that particular DNAE.

AAA Server must record the Accounting Records by mapping the NAS-IP-Address and NAS-Identifier (vNAS value) of each end-user received from NAS-Client based. This approach shall help to push dynamic-policies for end-user by including vNAS in Dynamic-Authorization messages towards DNAE which are part of DNAS. The following cases requires to update the information,

- Whenever NAS-Client (DNAE) is UP/DOWN in a given DNAS. - DNASs and DNAEs are located geographically in HSRP environment.

Earlier, whenever NAS-Client is going down is capable of sending Accounting Off or individual end-user Accounting Request with Acct-Status-Type with STOP to AAA Server. And also, Whenever NAS-Client is going down or Redundancy Roles are changed, old NAS-Client is going to send Accounting Off and New NAS-Client is going to send Accounting-On messages. In redundancy role exchange, old NAS-Client is used to generate Accounting-Request with Acct-Status-Type as STOP and new NAS-Client shall generate Accounting-Request with Acct-Status-Type as START for end-user accounting transactions. This is how AAA can close earlier transactions and maintain new transactions for end-user under HSRP scenarios.

Accounting Off messages are having significance role whenever NAS-Client is DOWN, this shall eventually help AAA Server to close all outstanding accounting transactions records that are maintained for end-users from each NAS-Client and with this approach, old NAS-Client no need to generate Accounting-Request with Acct-Status-Type with STOP for individual end-users.

6. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [RFC2234].

7. Acknowledgements

This template was derived from an initial version written by Pekka Savola and contributed by him to the xml2rfc project.

8. IANA Considerations

vNAS is a Virtual-NAS defined for DNAS and shall leverage the existing Radius NAS-Identifier attribute to include the vNAS value in Radius Messages. Based on review, may define a new attribute for vNAS in Radius Protocol.

9. Security Considerations

Because this document describes the problem space associated with the need for virtualization of networks in complex, large-scale, data-center networks, it does not itself introduce any security risks. However, it is clear that security concerns need to be a consideration of any solutions proposed to address this problem space. Solutions will need to address both data-plane and control-plane security concerns.

10. Informative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, DOI 10.17487/RFC1321, April 1992, <https://www.rfc-editor.org/info/rfc1321>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, DOI 10.17487/RFC2234, November 1997, <https://www.rfc-editor.org/info/rfc2234>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/info/rfc2866>.

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, DOI 10.17487/RFC2869, June 2000, <https://www.rfc-editor.org/info/rfc2869>.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, DOI 10.17487/RFC3162, August 2001, <https://www.rfc-editor.org/info/rfc3162>.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, DOI 10.17487/RFC3575, July 2003, <https://www.rfc-editor.org/info/rfc3575>.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, DOI 10.17487/RFC5176, January 2008, <https://www.rfc-editor.org/info/rfc5176>.

Authors' Addresses

Raghunadha Reddy Pocha (editor)
Cisco Systems
Cessna Business Park, Kadubeesanahalli
Bengaluru 560103
India

Phone: +91 9731 203 806
Email: pragredd@cisco.com

Chandrashekhar Jamadarkhani (editor)
Cisco Systems
Cessna Business Park, Kadubeesanahalli
Bengaluru 560103
India

Phone: +91 9972 039 140
Email: cjamadar@cisco.com

Satyanarayana Danda
Cisco Systems
Cessna Business Park, Kadubeesanahalli
Bengaluru 560103
India

Phone: +91 9741 732 155
Email: sdanda@cisco.com

Nishad M
Cisco Systems
Cessna Business Park, Kadubeesanahalli
Bengaluru 560103
India

Phone: +91 9482 538 306
Email: nism@cisco.com

Nagappa Chinnannavar
Cisco Systems
Cessna Business Park, Kadubeesanahalli
Bengaluru 560103
India

Phone: +91 9742 489 050
Email: nchinnan@cisco.com